**Statement of Ronald L Dick,**
**Director, National Infrastructure Protection Center**
**Federal Bureau of Investigation**
**before the**
**Senate Committee on Judiciary**
**Subcommittee for the Technology, Terrorism, and Government Information,**

**May 22, 2001**

Mr. Chairman, Ranking Member Feinstein, and members of the subcommittee, thank you for inviting me here today to testify about the General Accounting Office review of the National Infrastructure Protection Center. Let me start by stating that the GAO auditors who conducted the assessment carried themselves with the utmost professionalism throughout the eight-month audit of the Center. It was a pleasure to work with such bright, dedicated individuals.

Before addressing some of the issues raised by the GAO report, it is important to examine why the NIPC was created. In 1997 the President's Commission on Critical Infrastructure Protection finished its work and it was clear that the nation was woefully unprepared to deal with a major cyber attack. A new approach needed to be taken that combined the strengths of agencies across the U.S. government as well as innovative outreach to the private sector. Given that cyber intruders can be located anywhere and still reach their victims, this interagency center needed to have global capability. The center needed the legal authorities to be able to obtain records and analyze them for information. Finally, the center needed a response capability.

The NIPC can do all of the above and represents a cutting-edge approach to dealing with the difficult problem of computer intrusions. While housed at the FBI, the NIPC is an interagency Center. It currently consists of detailees from the following U.S. government agencies: FBI, Army, Office of the Secretary of Defense (Navy Rear Admiral), Air Force Office of Special Investigations, Defense Criminal Investigative Service, National Security Agency, General Services Administration, United States Postal Service, Department of Transportation/Federal Aviation Administration, Central Intelligence Agency, Department of Commerce/Critical Infrastructure Assurance Office, and a representative from the Department of Energy. Canada, the United Kingdom, and Australia also each have a detailee in the Center. In addition, the Center has had detailees from the Department of State, the National Aeronautics and Space Administration, and the U.S. Secret Service as well as state law enforcement officials detailed on a rotating basis from the Oregon State Police and the Tuscaloosa County (Alabama) Sheriff's Department.

The leadership of the Center is drawn from the law enforcement, defense, and intelligence communities. The Center is designed to combine and leverage the expertise of individuals throughout the government in an attempt to address this complex issue with the authorities granted to the FBI under the judicial oversight of the Department of Justice. Members of the interagency NIPC team have offices all over the United States and all around the world that are drawn upon to assist with cyber intrusion investigations.

Issues Raised by the Report

The NIPC was pleased that the report recognized the effectiveness of the NIPC's investigative program. The investigative program is currently handling over 1200 pending investigations. NIPC squads have been created in 16 FBI Field Offices: Washington D.C., New York, San Francisco, Chicago, Dallas, Los Angeles, Atlanta, Charlotte, Boston, Seattle, Baltimore, Houston, Miami, Newark, New Orleans, and San Diego. Other FBI Field Offices have smaller teams of one to five agents dedicated to working NIPC matters.

In the past year both on our own and working with our partners in law enforcement both nationally and globally, we have had some notable successes. A recent case exemplifies both the complex dimensions of the problem and the success we are having against it.

In the spring and summer of 2000, Michael Bloomberg, CEO of Bloomberg LP, reported receiving an extortion message stating that Bloomberg LP's., computer system had been compromised. According to complaints filed by the United States Attorney for the Southern District of New York, in the spring of 2000 two individuals from Kazakhstan, Ole Zezov and Igor Yarimaka, allegedly attempted to extort $200,000 from Mr. Bloomberg in exchange for providing information to Mr. Bloomberg as to how Zezov was able to infiltrate Bloomberg LP's, computer system. Mr. Bloomberg, working with law enforcement, agreed to meet with the alleged extortionists in London, United Kingdom, to resolve the matter and the meeting was held on August 10, 2000. The FBI worked with London Metropolitan Police authorities on the operation in which, according to the complaints filed, one UK officer posed as a Bloomberg LP executive and the other served as a translator. Shortly after the meeting Zezov and Yarimaka were arrested. The United States has requested their extradition. This operation demonstrates some of the NIPC's strengths. First, through the FBI's Legal Attaché program NIPC program agents could work closely with officers in London and Kazakhstan. The FBI currently has 44 Legal attaché offices that cover virtually every nation in the world. Second, the FBI is developing trust with the business community, as evidenced by the fact that Mr. Bloomberg notified the FBI about the extortion attempt and worked with law enforcement in the apprehension of the suspects.

The GAO commented favorably on the nationwide InfraGard initiative. All 56 FBI field offices now have active InfraGard chapters. Nationally, InfraGard has over 1200 members. It is the most extensive government-private sector partnership for infrastructure protection in the country, and is a service the FBI provides to InfraGard members free of charge for the American taxpayers. It particularly benefits small businesses which have no where else to turn for assistance. InfraGard expands direct contacts with the private sector infrastructure owners and operators and shares information about cyber intrusions and vulnerabilities through the formation of local InfraGard chapters within the jurisdiction of each of the 56 FBI Field Offices. The InfraGard program recently received the 2001 World Safe Internet Safety Award from the Safe America Foundation for its efforts. The success of the program is directly related to private industry's involvement in protecting its critical systems, since private industry owns almost all of the infrastructures. How has this worked in the real world? Last year an InfraGard member discovered a system compromise not only on its own machines, but on the machines of hundreds

of other companies. While the vulnerability was well known, the victims did not know they had been compromised. The NIPC discretely contacted the victim companies and those companies were able to remove the exploit tool from their systems. Last month InfraGard issued a sanitized report from one of its members to the rest of the membership regarding a new cyber incident.

Training is another NIPC strong point noted by the GAO. From scratch, NIPC interagency personnel developed a training program for not only FBI personnel but also for federal, state, local, and foreign law enforcement and security service personnel. The NIPC training unit has five core courses that concentrate on computer and network investigations. In the past three years over 1000 federal, state, local, and foreign law enforcement and security personnel have been trained in the NIPC's core courses. NIPC training courses are offered at the FBI academy at Quantico, Virginia, around the country at vendor facilities, and internationally at the International Law Enforcement Training Academies located in Budapest, Hungary, and Bangkok, Thailand. Over the past three years NIPC has provided training in its core and other courses for over 2,500 participants. The NIPC's training program complements training offered by the FBI's Training Division as well as training offered by other agencies and the National Cybercrime Training Partnership. Trained investigators are essential to our successfully combating computer intrusions. This training is paying rich dividends in investigative cooperation. For example, some of the officers from the Philippines, who with FBI agents successfully investigated the IloveYou virus in May 2000, had attended NIPC-sponsored training in Bangkok, Thailand.

Finally, the GAO notes that it was asked to determine "the purposes for which the NIPC used funding provided for fiscal years 1999 and 2000." The final report found that "the FBI appears to be funding the NIPC based on...congressional direction." It also found the NIPC used its funds to support its analysis and warning activities, investigation of computer crime, and outreach and information sharing with government and private sector entities.

In sum the report found many positive accomplishments by the interagency personnel assigned to the Center. This in particularly noteworthy given that the NIPC is only three years old (and just over two years old at the time of the GAO audit) and has faced many challenges as a startup organization. In that time, the Center has developed policies and procedures to help manage our nation's interagency infrastructure protection efforts. The NIPC has also had to develop policies and procedures for managing and coordinating investigative efforts in the FBI's 56 field divisions across the United States. Hundreds of personnel had to be recruited or transferred into the program. Most of these individuals had to be trained by a training program that itself was being developed from scratch.

Areas Cited for Improvement

Again, the NIPC's relatively recent formation should be kept in mind when discussing shortcomings in its performance. The NIPC is not a longstanding entity. Rather, it is a start-up organization less than three years old which has accomplished admirable results despite the fact that it began with no ready group of personnel to staff it. In addition, the NIPC operates in a milieu of federal agencies and for-profit entities, many of whom share aspects of its mission.

Yet despite these hurdles, the NIPC has grown successfully and continues to improve with rapid progress. Because of the speed with which the NIPC constantly matures, many of the GAO's recommendations have already been implemented.

Nevertheless, the NIPC considers it of the utmost urgency to address any remaining shortcomings identified in the GAO report. That does not mean that the NIPC accepts GAO's assessment of shortcomings in all cases. In reviewing each of the issues raised by the report, the NIPC sought to discern the underlying problems that led the GAO to perceive a shortcoming in a specific aspect of the NIPC's performance. Only by removing those underlying obstacles can the NIPC fully meet its own or others' expectations regarding its performance. Rest assured that the NIPC is already diligently working to fix problems identified in the report.

*Analysis*

The report identified the lack of strategic analysis as a major deficiency of the NIPC. The NIPC agrees that improvement is needed in this area and the Center has begun working on a plan to do so that incorporates the elements listed in the GAO report. The underlying causes for this perceived deficiency involve personnel shortfalls and management continuity, as noted in the GAO report. Both of these commodities have been in short supply in the NIPC's Analysis and Warning Section. First, regarding personnel resources, the NIPC requires a core cadre of analysts with the background and expertise to address the complicated questions regarding the infrastructure. In authorizing the expansion of the NIPC into a National Center, Presidential Decision Directive 63 directed components of the Executive Branch to "provide such assistance, information, and advice that the NIPC may request." While the Center is grateful to the partners who have provided assistance, the staffing resources provided from other Executive Branch components to the NIPC has been insufficient to allow the Center to fully meet the enormous analytical challenges of infrastructure protection. The NIPC counted on the expertise and contacts that would flow in from the other agencies to provide a core group around which the Center's analytic capability could be built. Instead the Center has relied almost exclusively on FBI intelligence specialists for its analytic staff. While these men and women are bright and dedicated, they are on a steep learning curve with regard to Critical Infrastructure Protection issues. Interagency detailees continue to be sought for the NIPC analytic effort. With them, the Center can produce more and better strategic analysis. None of this, however, should be construed as criticism of our Executive Branch partners. We recognize that acquiring and retaining highly skilled security personnel can be difficult and some agencies simply do not have the personnel available to send to the NIPC.

Second, the GAO report cited lack of planning with regard to the analysis effort as an NIPC shortcoming. This is not an issue of expertise but one of management. The leadership of the Analysis and Warning Section, which is responsible for the production of strategic analysis, is reserved for a Central Intelligence Agency officer. The unit chief positions in this Section responsible for the production and sharing of analytic products are reserved for the National Security Agency and the military components of the Defense Department, respectively. To date, the intelligence and defense communities have not consistently staffed these positions. This sporadic staffing has led to inconsistency in management. As I testify here today, the Section

Chief for Analysis and Warning has been on the job for only a month. The Unit Chief positions for both the Analysis and Information Sharing Unit and the Watch and Warning Unit, reserved for NSA and DoD, respectively, are currently vacant. The good news is that the new section chief is a CIA senior officer with sound strategic planning skills and extensive Intelligence Community experience who has made a personal commitment to the Center for at least two years. Similarly, we are in discussions with other agencies for high quality unit chiefs who will commit to remaining at the NIPC for at least two years.

In the short time that our Analysis and Warning Section chief has been onboard, we have already seen the rudimentary vision of what will soon be a fully articulated strategic plan. The key elements of this vision are threefold. First, rather than focusing on improving the use of alert functions in the midst of an attack, we will introduce forecasts of a nature similar to major warnings from the National Weather Service. Maybe we will only be able to achieve warning times equivalent to those for tornadoes at first but we want to be able to provide warnings more akin to those for hurricanes that have the same public safety and economic effect upon all aspects of an affected portion of society. Highly respected analysis -- both technically sound and prudently objective -- is essential. It is not only the hallmark of good threat warning but also the foundation for our enhanced threat and vulnerability analysis program that is better tailored to the particular needs of NIPC customers and partners. Second, we want this analysis to be not only stronger in content but broader in scope. We must increasingly address, for instance, more threatening case of integrated cyber and hard target attacks on our critical infrastructures. Finally, in order to achieve this vision, we must have a more proactive partnership with intelligence collectors. I understand that the goals in this vision are bold and they will not be easy or quickly reached but we must start somewhere.

*Warnings*

The report also criticized the NIPC Warning process by stating that most of the warnings concerned attacks that were already underway. This criticism is based on the fast-moving virus model, in which the virus is already in the wild causing damage before it is recognized and warnings can be issued. Specific prediction of how and when a virus or malicious code is unleashed in the information age, which to date have been typically released by lone wolf hackers, is very difficult. However, the NIPC recognizes that the cyber threat environment is much broader than just viruses and NIPC warning products must address the full gamut of those threats, ranging from hacker exploits to system vulnerabilities.

The NIPC has issued a number of warning products that preceded incidents or prevented them entirely by alerting the user community to a new vulnerability or hacker exploit before acts are committed or exploits used on a widespread basis. The Center has had particular success in alerting the user community to the presence of Denial of Service tools on the network and has in some cases provided a means to discover the presence of tools on a network. For example, in December 1999 the NIPC released a warning message along with a tool to allow users to find the presence of three specific denial of service tools on their systems. This is something never before done by the government for the user community and occurred over a month before the Distributed Denial of Service Attacks of February, 2000. The NIPC's work with private

companies has been so well received that the trade group Systems Administrators and Network Security Organization (SANS) awarded their yearly Security Technology Leadership Award to members of the NIPC's Special Technologies Applications Unit. Moreover, we modified these detection tools as we learned about modifications in the denial of service tools by the attackers.

In March 2001, we were commended by the Financial Services Information Sharing and Analysis Center (ISAC) for our advisory on e-commerce vulnerabilities (NIPC Advisory 01-003). This advisory, coupled with our press conference on March 8, 2001, stopped over 1600 attempted exploitations by hackers.

A better understanding of vulnerabilities is a key enabler to improving warning. Our Analysis and Warning Section is increasing its attention not only to the vulnerability of entire infrastructures but also to the vulnerabilities of individual products that are proliferated widely within those infrastructures. We are doing that through strengthened dialogue with public sector agencies, such as GSA, as well as private sector organizations and the Federally-Funded Research and Development Centers.

The report also states that the NIPC is not integrated into national security warning procedures. In fact, the NIPC is integrated into national level warning systems both through structures established by the National Security Council and by other agencies. NIPC looks forward to working with the White House on warning issues.

Notably, the GAO report did not recommend that the analysis and warning missions be moved out of NIPC. The initial reasoning for placing the NIPC within the FBI remains sound. The NIPC, under the authority of the FBI, is the only locus where law enforcement, counterintelligence, foreign intelligence, and private sector information may be lawfully and collectively analyzed and disseminated, all under well-developed statutory protections and the oversight of the Department of Justice. NIPC Advisory 01-003 and its companion NIPC Advisory 00-060, issued on March 8, 2001 and December 1, 2000, respectively, both on e-commerce vulnerabilities, are examples of warnings which effectively combine law enforcement, intelligence, and private sector information with the NIPC's warning mission. They reflect the balance of information dissemination to the public with an ongoing law enforcement investigation, achieving both goals in the public's interest.

*Information Sharing*

The report raises issues with regard to information sharing, both with respect to the NIPC sharing information with other entities and with regard to outside entities sharing information with the NIPC. There is a perception among some that the NIPC withholds information that would allow users to protect themselves based on law enforcement considerations in certain situations. This is emphatically not the case. The NIPC routinely shares information with the public and private sectors so as to allow them to better protect themselves. That does not mean that information is broadcast across the news media in every instance. While public statements are the best alternative in some cases, in other cases the NIPC has approached victim companies or government agencies privately. In many cases a tiered approach is taken so that information with the appropriate level of detail reaches the right audiences. This is particularly important in

instances where a company may have fallen victim to a well-known vulnerability. Private notification allows the company to repair the breach without publicity. If the NIPC finds that despite issuing an advisory, the problem persists or grows, then that advisory may be reissued. Such was the case with the e-commerce vulnerability advisory discussed above.

The NIPC has a variety of products to inform the private sector and other domestic and foreign government agencies of the threat, including: alerts, advisories, and assessments; biweekly *CyberNotes*; monthly *Highlights*; and topical electronic reports. These products are designed for tiered distribution to both government and private sector entities consistent with applicable law and the need to protect intelligence sources and methods, and law enforcement investigations. For example, *Highlights* is a monthly publication for sharing analysis and information on critical infrastructure issues. It provides analytical insights into major trends and events affecting the nation's critical infrastructures. It is usually published in an unclassified format and reaches national security and civilian government agency officials as well as infrastructure owners. *CyberNotes* is another NIPC publication designed to provide security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices. It is published twice a month on our website (www.nipc.gov) and disseminated in hardcopy to government and private sector audiences.

To better share information the NIPC has spearheaded an aggressive outreach effort and in fact has formed an entire unit dedicated to that task. NIPC officials have met with business, government, and community leaders across the United States and around the world to build the trust required for information sharing. Protection of business information and privacy interests are both stressed in NIPC internal deliberations and with business, government and community leaders. Most have been receptive to information sharing and value the information received from the NIPC. Others have expressed reservations due to lack of understanding or perhaps confidence in the strength of the exemptions found in the Freedom of Information Act, concerns about whether the Justice Department would pursue prosecutions at the expense of private sector business interests, and simple reluctance to disclose proprietary information to any entity beyond their own control or beyond the direct control of the NIPC. We have moved aggressively to address these concerns and will continue to do so.

The NIPC is continuing to reach out to the Information Sharing and Analysis Centers (ISACs). While in some cases the relationship may have started off slowly, the momentum for increased information sharing is steadily growing. For example, the NIPC worked with the Financial Services ISAC on the advisory issued on March 8, 2001 concerning vulnerabilities in e-commerce systems. Just as important, the NIPC is receiving reports from member companies of the ISACs. The NIPC has proven to these companies that it can properly maintain their information and can provide them with useful information. It is because of such reporting that the investigative caseload of the NIPC is burgeoning and more warning products are being issued each year.

One example bears discussion. The North American Electric Reliability Council (NERC) serves as the electric power ISAC. The NIPC has developed a program with the NERC for an

Indications and Warning System for physical and cyber attacks. Under the program, electric utility companies and other power entities transmit incident reports to the NIPC. These reports are analyzed and assessed to determine whether an NIPC alert, advisory, or assessment is warranted to the electric utility community. Electric power participants in the program have stated that the information and analysis provided by the NIPC back to the power companies make this program especially worthwhile. NERC has recently decided to expand this initiative nationwide. This initiative will serve as a good example of government and industry working together to share information and the Electrical Power Indications and Warning System will provide a model for the other critical infrastructures.

With the assistance of the North American Electric Reliability Council (NERC), the NIPC conducted a six-month pilot program and a series of workshops to familiarize participants with the program's operating procedures. Both the pilot and the workshops included hands-on table-top exercises that required program participants to work through simulated scenarios dealing with credible cyber and physical attacks directed against the power industry. In the summer of 2000, a half-day table-top exercise was held for companies in NERC's Mid-Atlantic region allowing them to role-play in responding to simulated incidents pre-scripted by NIPC and company representatives. Since October 2000, the NIPC supported by NERC conducted three workshops in Columbus, Dallas, and Las Vegas in order to provide program participants with hands-on experience in responding to attacks against the electric power grid. Eventually, the NIPC will strive to have similar models and exercises for all the infrastructures.

*Interagency Cooperation*

Regarding sharing information within the government, PDD-63 mandates that government agencies will share information with the NIPC. The NIPC has established effective information sharing relationships across the U.S. Government. These arrangements are not always codified in formal interagency agreements or Memoranda of Understanding, but the important point is that they are working. The NIPC has also formed an Interagency Coordination Cell at the Center which holds monthly meetings. To date, the IACC's growing membership has risen to approximately 26 government agencies that meet on a monthly basis to include representation from NASA , U.S. Postal Service, Air Force Office of Special Investigations (AFOSI), U.S. Secret Service, U.S. Customs, Departments of Energy, State and Education, and the Central Intelligence Agency to name a few. The cell works to deconflict investigative matters among agencies and assists agencies in combining resources on matters of common interest.

The IACC's accomplishments to date include the formation of several joint investigative task forces with member agencies participating, and approximately 20 separate instances of joint investigations of member agencies being initiated as a direct result of IACC meetings, information sharing and participation. In one case that took place approximately 2 months ago, an IACC member agency provided timely sensitive source information to the appropriate authorities which prevented the planned intrusion and compromise of another government agency's computer system and the preservation of critical log data used for the ensuing investigation.

The IACC's good work continues, as its members are currently working on the establishment and development of a database which would serve as a source of computer intrusion information compiled from member agency investigations to facilitate other investigations. It is also working on the setup and administration of a dedicated virtual private secure network for member agencies to communicate vital infrastructure protection and computer intrusion information for immediate emergency response situations, in addition to dissemination of routine but sensitive information.

After the FBI, the Department of Defense (DoD) has the second largest interagency contingent in the NIPC. The Deputy Director of the NIPC is a two-star Navy Rear Admiral, the Executive Director is detailed from the Air Force Office of Special Investigations, the Assistant Section Chief for Training, Outreach and Strategy is detailed from the Defense Criminal Investigative Service, the head of the NIPC Watch is reserved for a DoD military officer, and the head of the Analysis and Information Sharing Unit is reserved for an National Security Agency Manager. NIPC works particularly closely with the Department of Defense (DoD) through liaison with the Joint Task Force-Computer Network Operations (JTF-CNO). NIPC stays in close contact with its JTF-CNO counterparts, providing mutual assistance on intrusion cases into DoD systems, as well as on other matters. NIPC alerts, advisories, and assessments are routinely coordinated with the JTF-CNO prior to release to solicit JTF-CNO input. On several occasions, the NIPC and JTF-CNO have coordinated and issued joint advisories on the same matter. An initiative has also been tested in which Watch personnel from the NIPC work side by side with JTF-CNO officers. Under this initiative, NIPC and JTF-CNO personnel will spend time standing watch at the other's operations center. As of this date, the NIPC has detailed Watch personnel to the JTF-CNO for day-long exchange tours. We expect to have an increase of cross details between the two organizations which should enhance mutual understanding of watch and warning procedures.

*Relationship with CERT/CC, FedCIRC and Anti-Virus Community*

The NIPC and the Computer Emergency Response Team (CERT) at Carnegie Mellon University have formed a mutually beneficial contractual relationship. The NIPC receives information from the CERT (including advance Special Communications about impending CERT advisories, which CERT seeks NIPC input on, and weekly intrusion activity information) that it incorporates into strategic and tactical analyses and utilizes as part of its warning function. The NIPC's Watch and Analysis units are routinely in telephonic contact with CERT/CC and the anti-virus community for purposes of sharing vulnerability and threat information on a real-time basis. CERT/CC input is often sought when an NIPC warning is in production. The NIPC also provides information to the CERT that it obtains through investigations and other sources, using CERT as one method for distributing information (normally with investigative sources sanitized) to security professionals in industry and to the public. The Watch also provides the NIPC Daily Report to the CERT/CC via Internet e-mail. On more than one occasion, the NIPC provided CERT with the first information regarding a new threat, and the two organizations have often collaborated in putting information out about incidents and threats.

The NIPC has an excellent relationship with the General Services Administration's Federal Computer Incident Response Center (FedCIRC). FedCIRC and the NIPC are both crucial to effective cyber defense but serve different roles to the Federal community. When an agency reports an incident, FedCIRC works with the agency to identify the type of incident, contain any damage to the agency's system, and provide guidance to the agency on recovering from the incident. FedCIRC has detailed a person to the NIPC Watch Center. In addition, the NIPC sends draft alerts, advisories, and assessments on a regular basis to FedCIRC for input and commentary prior to their release. NIPC and FedCIRC information exchange assists both centers with their analytic products. The NIPC and FedCIRC are currently discussing ways to improve the flow of information between the two organizations and encourage federal agency reporting of incident information to the NIPC.

*Emergency Law Enforcement Services Sector*

The NIPC has critical infrastructure sector responsibilities. The Department of Justice/FBI is the Sector Lead Agency with regard to Emergency Law Enforcement Services (ELES). The NIPC serves as program manager for this function at the request of the FBI. Just after the GAO finished collecting its data, the NIPC completed the Emergency Law Enforcement Services Sector Plan. Working with law enforcement agencies across the United States, the NIPC conducted a sector survey and used the results of this survey to draft a sector report. ELES was the first completed sector report under PDD-63 and was delivered to the White House on March 2, 2001. The ELES Plan and accompanying guide were presented by ELES Sector Coordinator Sheriff Patrick Sullivan of Colorado to the Partnership for Critical Infrastructure Security in Washington, D.C., in March, 2001. At that forum the ELES Plan was held up as a model for the other sectors. The NIPC also sponsored the formation of the Emergency Law Enforcement Services Sector forum, which meets quarterly to discuss issues relevant to sector security planning.

*Monitoring Reconstitution*

Monitoring reconstitution was another area noted by the report. The mission of the NIPC (in priority order) is to detect, deter, assess, warn (users), respond to, and investigate unlawful acts involving computer and information technologies and unlawful physical and cyber acts that threaten or target our critical infrastructures. The NIPC supports the reconstitution of essential services as quickly as possible and will work with the private sector so that reconstitution does not needlessly destroy information and evidence that can lead to the parties who caused the damage. The objective of the Key Asset Initiative is to develop and maintain a database of information concerning "key assets" within each FBI Field Office's jurisdiction as part of a broader effort to protect the critical infrastructures against both physical and cyber threats. To date, the NIPC has identified 5,596 "key asset" entities. This initiative will assist in monitoring reconstitution efforts by providing a better understanding of the asset's location, importance, and to provide a basis for contingency planning and prudent crisis management.

The NIPC has experience in establishing a command post to monitor possible reconstitution efforts. One of the functions of the Y2K Command Center, managed by the NIPC

for the FBI, was to monitor reconstitution of systems should outages have occurred. The Y2K command center was modeled on the basic Joint Operations Center format used by the FBI for crisis management. During the Y2K rollover, NIPC operated around-the-clock for six days, with full shifts of 49 personnel per shift, with cells responsible for executive management, investigations, intelligence, watch and warning, legal affairs, technical functions, administration, and media relations. The NIPC also detailed 6 personnel to the Y2K Information Coordination Center managed by the White House.

In the event of a national-level set of intrusions into significant systems, the NIPC has developed specific crisis response planning. Should a crisis occur, the NIPC will form a Cyber Crisis Action Team (C-CAT) to coordinate response activities using the facilities of the FBI's Strategic Information and Operations Center (SIOC). The team will have expert investigators, computer scientists, analysts, watch standers, and other U.S. government agency representatives. Part of the U.S. government team might be physically located at FBI Headquarters and part of the team may be electronically connected from anywhere in the world. The C-CAT will immediately contact FBI Field Offices and other agencies responsible for the jurisdictions where the attacks are occurring and where the attacks may be originating. The C-CAT will continually assess the situation and support/coordinate investigative activities, issue updated warnings, as necessary, to all those affected by or responding to the crisis. The C-CAT will then coordinate the investigative effort to discern the scope of the attack, the technology being used, and the possible source and purpose of the attack. During the investigation, the C-CAT will monitor reconstitution activities. We expect that more specific guidance regarding the monitoring of reconstitution will be forthcoming in version 2 of the National Plan for Information Systems.

International Activities

The report touches only briefly on the vast array of NIPC international activities. A typical cyber investigation can involve victim sites in multiple states and often many countries, and can require tracing an evidentiary trail that crosses numerous state and international boundaries. Even intrusions into U.S. systems by a perpetrator operating within the U.S. often require international investigative activity because the attack is routed through Internet Service Providers and computer networks located outside the United States. When evidence is located within the United States, the NIPC coordinates law enforcement efforts which might include: subpoenaing records by FBI agents, conduct of electronic surveillance, execution of search warrants, seizing and examining of evidence. We can do none of those things ourselves overseas to solve a U.S. criminal case. Instead, we must depend on the local authorities to assist us. This means that effective international cooperation is essential to our ability to investigate cyber crime.

International investigations pose special problems. First, while the situation has improved markedly in recent years, many countries lack substantive laws that specifically criminalize computer crimes. This means that those countries often lack the authority not only to investigate or prosecute computer crimes that occur within their borders, but also to assist us when evidence might be located in those countries. Moreover, the quickly evolving technological aspects of these investigations can exceed the capabilities of local police forces in

some countries. Finally, even when countries have the requisite laws and have developed the technical expertise necessary to conduct cyber investigations, successful investigation in this arena requires a more expeditious response than has traditionally been the case in international matters, because electronic evidence is fleeting and, if not secured quickly, can be lost forever.

The NIPC is working with its international partners on several fronts. The first area consists of outreach activities designed to raise awareness about the cyber threat, encourage countries to address the threat through substantive legislation, and provide advice on how to organize to deal with the threat most effectively. Almost weekly the NIPC hosts a foreign delegation to discuss topics ranging from current cases to the establishment of NIPC-like entities in other nations. Since the NIPC was founded, Australia, Japan, Israel, the United Kingdom, Canada, Germany, and Sweden have all formed interagency entities like the NIPC. The NIPC has established Watch Center connectivity with watch centers in Australia, Canada, the United Kingdom, Sweden, and New Zealand. The NIPC has briefed visitors from the United Kingdom, Germany, France, Norway, Canada, Singapore, Bulgaria, Estonia, Latvia, Japan, Denmark, Sweden, Israel, and other nations over the past year regarding critical infrastructure protection issues.

Abroad, the FBI's Legal Attaches (Legats) are often the first officials contacted by foreign law enforcement should an incident occur. We are providing training to our Legats on how to coordinate computer intrusion and infrastructure protection matters with us to make them more effective. In addition, NIPC personnel are in almost daily contact with Legats around the world to assist in coordinating requests for information.

In order to help make our foreign partners more capable to assist our international investigations and to address cyber crime within their own countries, the NIPC has also provided training to investigators from several nations. Much of this training takes place at the International Law Enforcement Academies in Budapest, Hungary and Bangkok, Thailand. In addition, a small number of select international investigators receive training in NIPC sponsored classes in the United States. The NIPC also holds workshops with other nations to share information on techniques and trends in cyber intrusions.

Another international initiative that the NIPC has been involved in is the G-8's High-Tech Crime Subgroup of the G-8 “Lyon Group.” A representative of the NIPC serves as a member of the United States delegation to the Subgroup, which has been considering several issues concerning international cyber crime investigations, international training conferences, review of legal systems in G-8 countries, and the development of the G-8 principles on transborder access to stored computer data.

The 24/7 high-tech points of contact network was established in March 1998. Each of the G-8 countries identified a point of contact for law enforcement in each of their respective countries. These contacts are required to be available twenty-four hours a day, seven days a week, in order to respond to requests for assistance in important high-tech crime investigations in which electronic evidence may either be altered or destroyed.

Conclusions

The report raises a number of issues. Many of the issues raised in the report have easy remedies and in fact have been or are in the process of being fixed. There is a lot right with the NIPC, and it was pleasing to see much of that reflected in the GAO's audit. We will keep in contact with the committee regarding our efforts to respond to the issues raised by this report.

Thank you.